NIST Cryptograph Standards Plans

Bill Burr

Group Manager

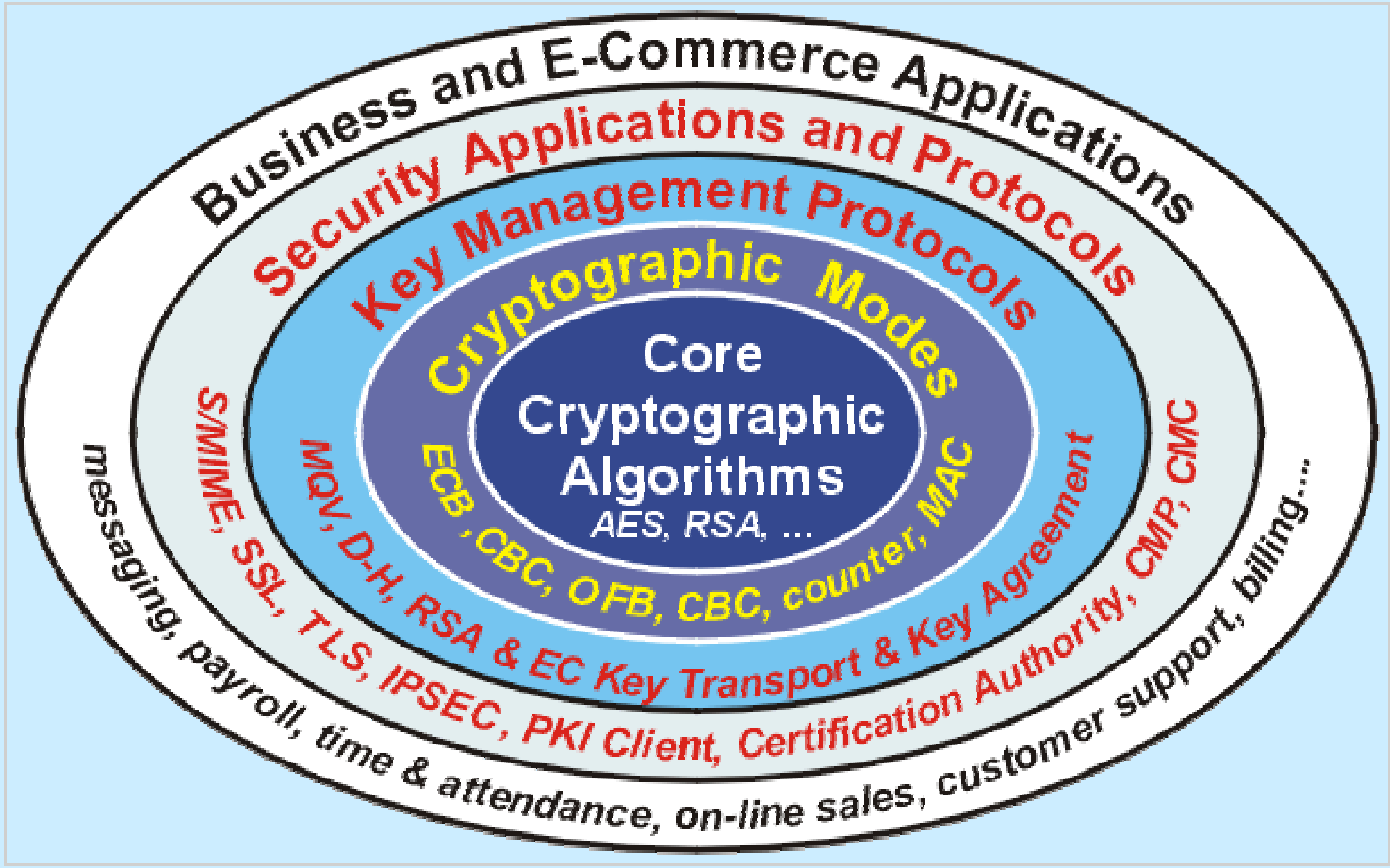
william.burr@nist.gov

Jan 30, 2001

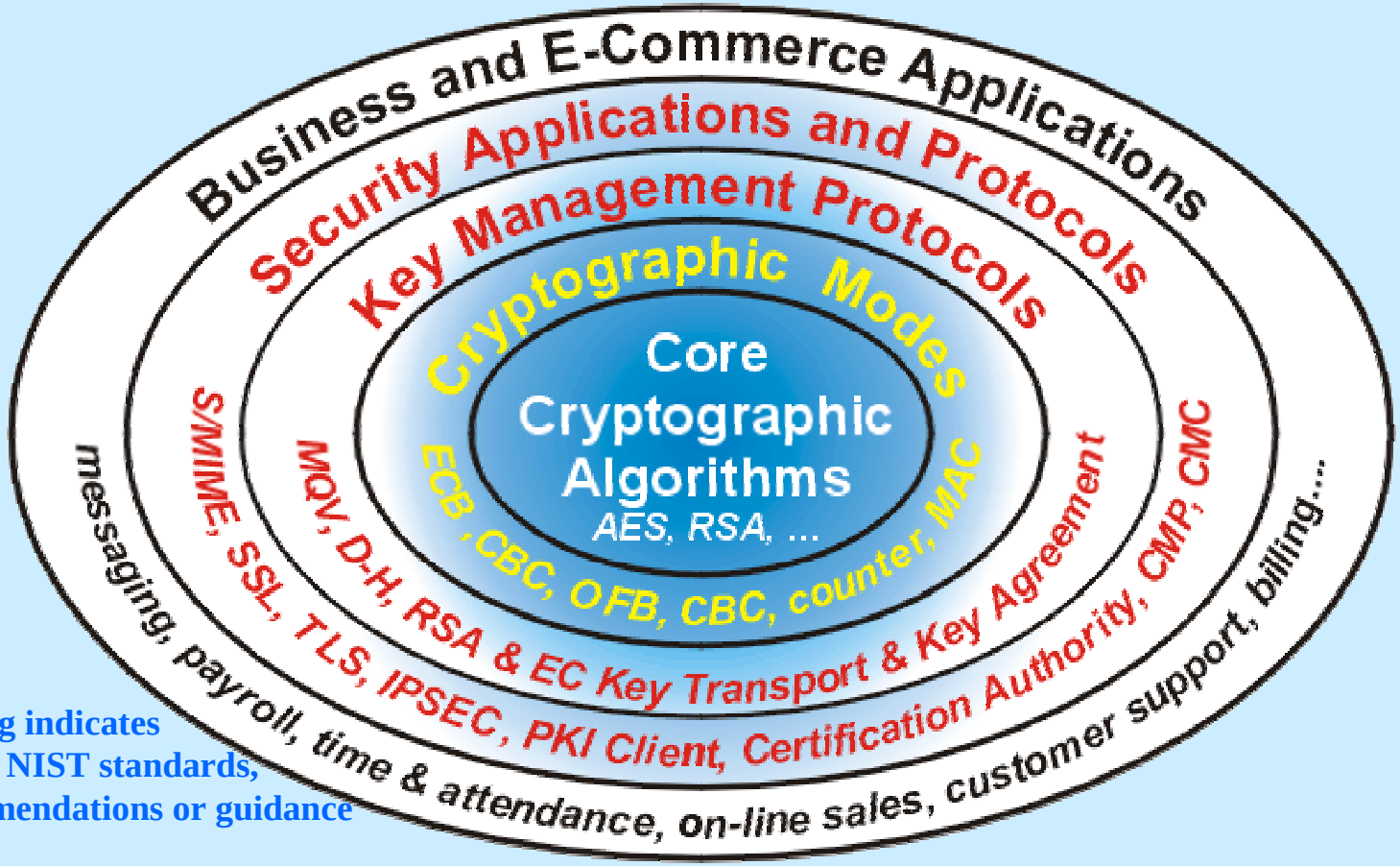
Cryptographic Standards Toolkit

- Basic Cryptographic Algorithms for
  - encryption
  - key management
  - authentication and signatures
- Modes and Protocols
  - encryption modes
  - key management
- Comparable strengths
  - crypto is no stronger than its weakest link
  - very high security alternatives

Cryptographic Security Core

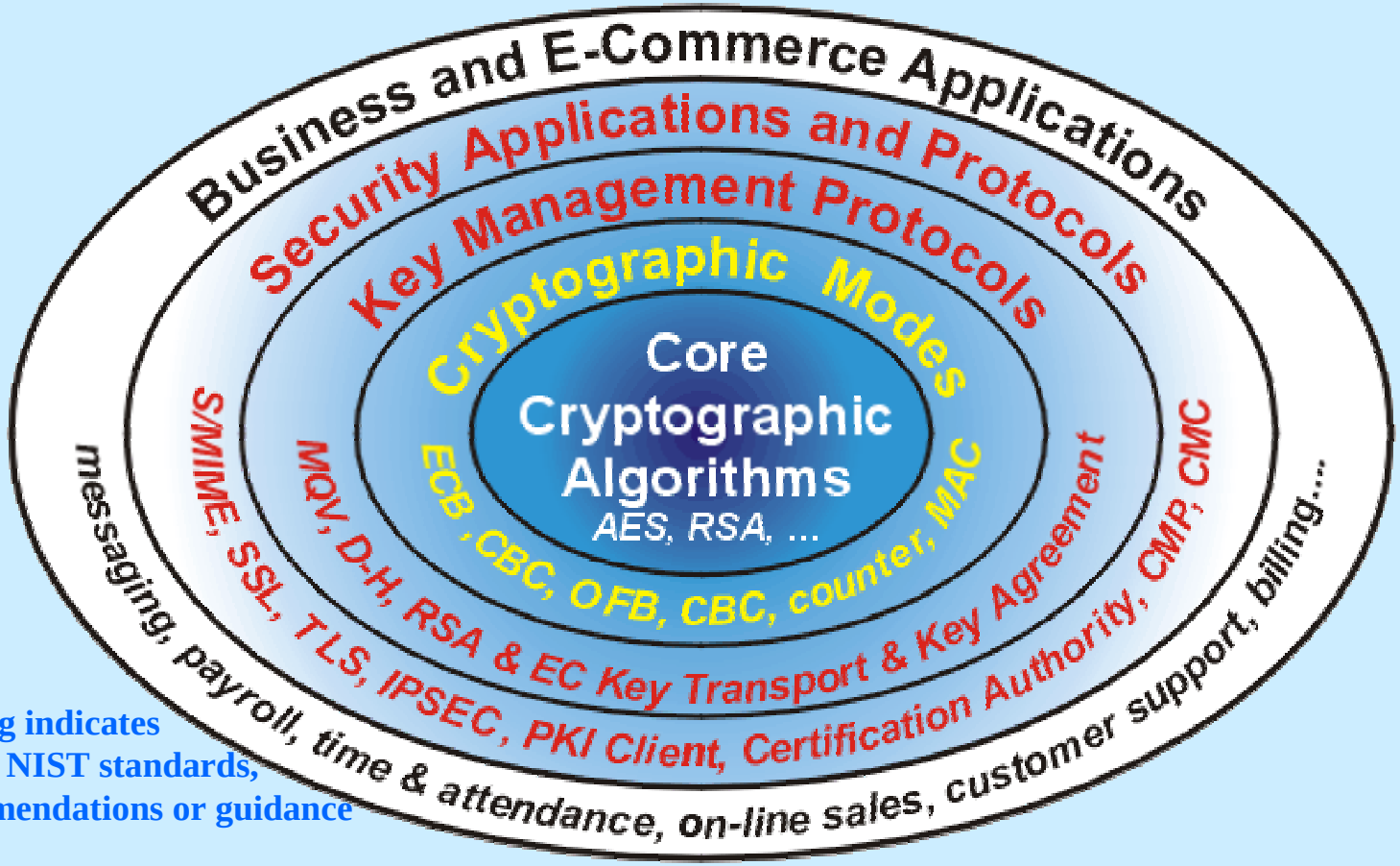


Overall, Where is NIST Now?



Shading indicates area of NIST standards, recommendations or guidance

Where does NIST Want to go?



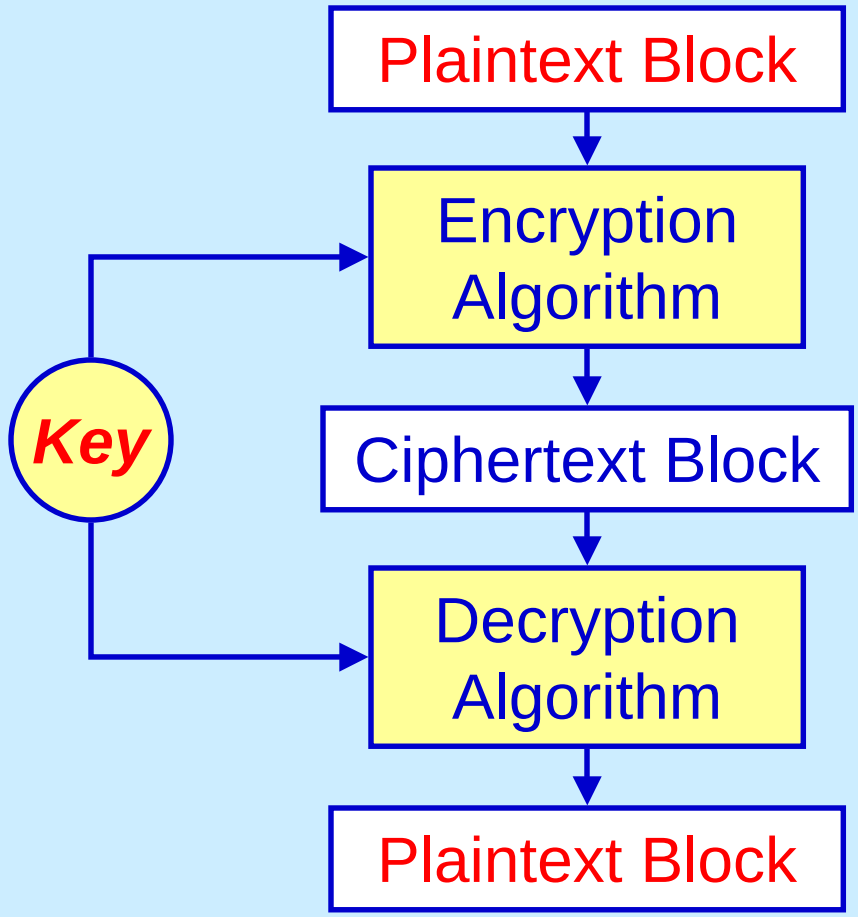
Shading indicates area of NIST standards, recommendations or guidance

Algorithm Categories

- Symmetric key
  - encrypt and decrypt using same key
- Hash
  - turn long message into smaller fixed “message digest”
- Message Authentication Code (MAC)
  - uses a key to authenticate a message
- Public (Asymmetric) key
  - two related keys: one public, other private
  - digital signatures and key management
  - Factoring, discrete log, or elliptic curve based

Symmetric Key Block Cipher

- Encrypt & Decrypt with the same key
- Fast workhorse
  - Used for most message and file encryption
- Used in a variety of "Modes of operation"
  - different security and other properties



Symmetric Key Strength

- A “good” symmetric key algorithm is one where brute force key exhaustion is the best attack
  - 56-bits broken by key exhaustion circa 1997
    - parallel processing attack is easy
- Moore’s Law:
  - computer power per $ doubles in 18 months
    - therefore can break one additional bit every 18 months
- 2^{128} is a very big number
  - a machine that cracks 56-bits in a second takes 149 trillion years to crack a 128-bit AES key

Symmetric Key Standards

- Data Encryption Standard (DES), FIPS 46-3
  - 56-bit, 64-bit block, vulnerable to key exhaustion
- Skipjack (Escrowed Encrypt. Std) FIPS 185
  - 80-bit, 64-bit block, unpopular
- Triple DES, FIPS 46-3
  - 112-bit strength, 64-bit block, strong, slow
- Advanced Encryption Standard (AES)
  - 128, 192 & 256-bit keys
  - 128-bit block size
  - strong to very strong and fast

Modes of Operation

- Specify different ways to use sym. key alg.
- FIPS 81: DES modes of operation
  - 4 basic modes, widely used
  - specific to 64-bit DES/Skipjack block size
- AES Modes of Operation
  - Part I - soon
    - generalize 4 DES modes for other block sizes
    - add counter mode (for higher performance)
  - Part 2 - later
    - consider new, “parallizable” and “authenticating” modes
      - 2nd workshop planned Aug. 2001

Cryptographic Hash Algorithms

- Reduces a message to a fixed size *message digest*
  - used for authentication and integrity
    - digital signatures, with public key algorithms
    - message Authentication codes (HMAC) with secret key
- "Birthday" attack
  - n-bit sym. key and a 2n-bit hash roughly equivalent

Hash Standards

- FIPS 180-1
  - SHA-1 160-bit hash; preferred hash algorithm today
- FIPS 180-2 planned to include larger hash fields
  - SHA-1 (160-bit)
  - SHA-256
  - SHA-384
  - SHA-512

Msg. Authentication Codes

- Current DES-MAC (FIPS 113 & FIPS 81)
  - 64-bit MAC
    - only 2^{32} work factor for birthday attacks - not strong enough for many applications
- HMAC
  - hash of message concatenated to secret key
  - allow different hash functions and sizes
- AES MAC ???
  - would have 128-bit MAC, 2^{64} work factor
  - other modes that offer encryption, authentication & integrity?

Digital Signature Standards

FIPS 186-2

- DSA (X9.30) - defined for ≤ 1k modulus
- RSA (X9.31)
  - PKCS#1 vs. X9.31 incompatibilities
- ECDSA (X9.62)
- all 3 Require SHA-1 160-bit message digest

- FIPS 186-3
  - Add larger keys for DSA
  - Require > 160-bit hashes for big keys
  - Add PKCS #1

Accelerated Key Management Effort

- Key management is the missing part
  - The most difficult part
  - Substantial guidance & protocol component
- Workshop held Feb 2000
  - Scheme
  - Guideline
- Accelerated effort
  - Two working groups with NSA
  - Support Contract

Key Management Standard

- Diffie-Hellman (X9.42) - key agreement
- RSA (X9.44) - key transport
- EC-Diffie-Hellman - key agreement
- Two-tier FIPS Planned
  - *Scheme* states crypto algorithm primitives
  - *Guidance document* states protocols and general guidance
    - key management protocols are numerous and sometimes complex
      - embodied in apps like SSL/TLS, S/MIME, IPSEC, etc.
    - May be NIST Recommendation rather than FIPS

Comparable Strengths

Size in bits

Sym. Key	56	80	112	128	192	256
Hash	160		256		384	512
MAC	160		256		384	512
RSA/DSA	512	1k	2k	3k	7.5k	15k
EC	160		224	256	384	512

Sym. Key: Symmetric key encryption algorithms
MAC: Message Authentication code
Pub. Key: Factoring or discrete log based public key algorithms
EC: Elliptic Curve based public key algorithms
White background: current FIPS (at least for signatures)
Yellow background: planned FIPS

Speed vs Strength

- Symmetric Key
  - slowdown with bigger key often less than linear
    - 256-bit AES 40% slower than 128-bit AES
- Hash
  - probably about linear?
- RSA
  - public key operations: $O(k^2)$ steps
  - private key operations: $O(k^3)$ steps
  - key generation: $O(k^4)$ steps

NIST Crypto Standards Plans

<table>
<tr><th></th><th>56</th><th>80</th><th>112</th><th>128</th><th>192</th><th>256</th></tr>
<tr><td>Sym. Key</td><td>46-3</td><td>185</td><td rowspan="2">46-3</td><td colspan="3">AES FIPS</td></tr>
<tr><td>Modes</td><td colspan="2">81</td><td colspan="3">AES Modes</td></tr>
<tr><td>Hash</td><td colspan="2">180-1</td><td colspan="4">180-2</td></tr>
<tr><td>MAC</td><td colspan="6">HMAC FIPS</td></tr>
<tr><td>RSA, DSA,
EC-DSA</td><td colspan="2">186-2</td><td colspan="4">186-3</td></tr>
<tr><td>DH/RSA</td><td colspan="6" rowspan="2">Key Management FIPS:
Scheme and Guidance</td></tr>
<tr><td>EC-DH</td></tr>
</table>

White background: existing FIPS
Red background: discussion phase

Yellow background: draft in progress
Gray background, 2 stages, one to be done soon

FY2001

- Approval of
  - FIPS 140-2
  - AES FIPS
    - ISO-IEC JTC1 SC27 WG2 and X9 standards in works
  - HMAC FIPS
  - FIPS 180-2 (new Hash FIPS)
  - Revised DSS (FIPS 186-3) ?
    - bigger keys, PKCS #1
- Develop
  - AES Modes of Operation (Part 1)
    - 4 familiar modes + counter
- Start on
  - New Modes of Operation
  - Key Mgt. “Scheme” and Guidance
    - accelerated schedule

Other Areas for New Crypto FIPS

- Prime Number Generation
  - X9.80
- Random Number Generation
  - X9.82
  - NIST effort in RNG testing

More Information

- **Links**
  - Crypto Toolkit: http://csrc.nist.gov/encryption/
  - Encryption: http://csrc.nist.gov/encryption/tkencryption.html
  - HMAC: http://csrc.nist.gov/encryption/hmac/
  - Modes of Operation: http://csrc.nist.gov/encryption/tkmodes.html
  - Key Management: http://csrc.nist.gov/encryption/tkkeymgmt.html
  - AES: http://csrc.nist.gov/encryption/aes/
  - Crypto Module Validation http://csrc.nist.gov/cryptval/

- **Points of Contact**

Bill Burr	**william.burr@nist.gov**
FIPS 140: Ray Snouffer	**stanley.snouffer@nist.gov**
Crypto stds.: Elaine Barker	**ebarker@nist.gov**
PKI: Tim Polk	**wpolk@nist.gov**

Conclusion

- NIST is building a comprehensive cryptographic toolkit
  - strong security
    - Comparable strengths in different algorithms
  - assurance & validation testing
  - suitable for commercial use and COTS products
  - encourage industry participation

Questions